PAGE

100 Overview

The Commonwealth Accounting and Reporting System (CARS) security table determines user access to system features at the agency, user type, and user identification levels. Users may or may not be permitted to inquire into or update system files and tables.

200 Policy

The security table is controlled by the Department of Accounts (DOA). No other user in the Commonwealth is granted maintenance access to this table.

It is the responsibility of each agency's CARS Security Officer to ensure that adequate internal controls exist within that agency to prevent unauthorized access to online CARS data, and that each logon ID (identification number) is assigned to an individual, not to a group or section.

300 Establishing A CARS Logon ID

The steps required to establish a logon ID in CARS are described in this subsection. These procedures require involvement by agency personnel who are familiar with both CARS processing and agency internal controls. These steps require coordinated action between:

- the agency's CARS security officer,

- the agency's ACF2 security officer (to determine who is the ACF2 security officer for your agency, call the DIT security officer at 804/344-5822),

- your agency's Department of Information Technology (DIT) customer liaison,

- the DOA Data Base Administrator, and

- the DOA General Accounting Section.

Security planning is crucial due to the number of parties involved and the specific constraints on user access to both DIT's computers and CARS files. Plan to take initial action at least one month in advance of anticipated system access. To ensure prompt response to security access requests:

- Follow these procedures closely, and

- Utilize personal delivery or overnight delivery service (e.g., Federal Express) to route security documents.

Perform each of the steps in the procedures as listed.

301 COMPLETE Administrative Activities

Contact your Agency's Data Processing Department to determine if your agency has on-line access through existing agency hardware and communications lines to the Department of Information Technology. If you do not have a data processing staff or are not a customer of DIT, contact the DIT Customer Liaison staff at (804) 786-3932 for assistance.

300 Establishing A CARS Logon ID (Continued)

302 CARS Security Officers

- Review duties of CARS Security Officers in Subsection 401, "Duties of the CARS Security Officer."

- Identify CARS Security Officers for your agency.

- Complete and submit new Authorized Signatories Form (Form DA-04-121) according to CAPP Volume 1, Topic No. 20310, "Expenditures." Note that submission of the Authorized Signatories Form is not sufficient unless the CARS Security Officers on that form have been identified in accordance with Subsection 401, "Duties of the CARS Security Officer." This is only required if logon ID is a type 7 or 8 and the person is not currently listed on the form or if a new CSO has been named.

303 Logon ID Request Form - IBM Technology

(A copy of this form appears as Exhibit 1)

- Before establishing a new logon ID in CARS, this form must be submitted to and approved by the DOA Data Base Administrator (DBA) in accordance with Subsection 600, "General Coding Requirements," if it is a "Data Entry" logon ID. This form must be submitted to DIT if it is an "Inquiry" logon ID.

- This form must be signed by the agency's ACF2 Security Officer.

- Logon IDs are established with passwords which are the same as the logon ID's. <u>The agency must change each password before continuing to the next step</u>. For instructions on how to change a password, consult your ACF2 Security Officer.

304 CARS Security Table Maintenance Form

(A sample copy of this form appears in Exhibit 2).

- A supply of these forms can be obtained by sending a written request to DOA Administrative Services.

- Determine the types of CARS users within the agency. Security access under user types 7 (agency approval) and 8 (data entry and approval) is limited to those individuals listed on the agency's Authorized Signatories Form (DA-04-121). These individuals are delegated authority by the Agency Head to approve and release expenditure documents to DOA for processing.

- Complete the CARS Security Table Maintenance Form (DA-04-197) using the Security Table Maintenance Summary (Reference Exhibit 2).

- Submit the CARS Security Table Maintenance Form to DOA.

- Upon completion of the addition, deletions or changes, a confirmation copy will be returned to the agency. Please review this copy to ensure that the changes made to the security table record are as you intended.

- If an error is noted on the security form, a new form must be completed and resubmitted to DOA.

- DOA recommends filing all blank Security Table Maintenance Forms and copies of authorized forms in a locked file cabinet accessible only to the CARS Security Officer.

400 CARS Security Officer (CSO)

Each agency is responsible for selecting two key individuals to be designated as CARS Security Officers (CSOs). In addition, each agency head will serve as an ex officio CARS Security Officer.

401 Duties of the CARS Security Officer

The primary purpose of the CARS Security Officer is to control, within DOA constraints, an agency's access to CARS by its personnel. In addition, this position serves as the key liaison between DOA and all agency personnel who interact with CARS (including the ACF2 Security Officer), submit data to CARS, and hold an interest in CARS reports. The CARS Security Officer is responsible for the following at a minimum.

- Maintenance of a comprehensive intra-agency system of internal control over both online and offline access to CARS tables and files, within the constraints described in this section.

- Compliance with DIT Directive 92-1, System Access Control, inclusive of obtaining and filing completed Information Security Access Agreements from each CARS user with a logon ID beginning with "ACT." A completed Information Security Agreement must be obtained from the user prior to transmitting the Logon ID Request Form - IBM Technology (DIT03-001) for an "ACT" logon ID. The CSO, by signing the Request Form, is attesting to the completion of this requirement. These agreements are to be filed at the user agency and they must not be transmitted to DOA.

- Maintenance of a current mailing address on the DOA mailing list,"CARS Security Officers."

Requests for additions or changes to the DOA mailing list for CARS Security Officers must meet the following specifications.

Address:	**U. S. Mail**
	Table Maintenance/General Accounting
	DEPARTMENT OF ACCOUNTS
	Post Office Box 1971
	Richmond, VA 23215-1971
	Other Delivery
	Table Maintenance/General Accounting
	DEPARTMENT OF ACCOUNTS
	Third Floor, Monroe Building
	101 North 14th Street
	Richmond, VA 23219
Format:	Request must be typed on agency letterhead.
Authorization:	Must be signed in full by CARS Security Officer.
Data Required:	Agency Name and Number
	CSO Name and Signature
	Agencies for the Which the Change is Effective
	Effective Date
	Mailing Address

- Receipt and dissemination of documentation to all agency operating personnel requiring CARS policies and procedures.

400 CARS Security Officer (CSO) (Continued)

401 Duties of the CARS Security Officer (Continued)

- Notation of the primary CSO and a secondary CSO on the agency's signature card. This will be accomplished by typing or printing "/CSO" after the individual's title on the signature card. Due to the critical nature of the CSO function and the need to maintain continuity in agency CARS operation, DOA requires the naming of a primary and a secondary CSO on each signature card. Also, the agency head is empowered to act as a CARS Security Officer, whether or not CSO designation appears on the agency signature card.

  LIMITATION: Two designated CSOs per agency number, not including the agency head.

  EXAMPLE: If the Accounting Manager is designated a CSO, the person's name and signature must appear on the agency's signature card with the "Title" designated:

<div align="center">

Accounting Manager/CSO

</div>

402 CSO Scope of Authority

The CSO may authorize access, within DOA constraints, to CARS, for the agency number that corresponds to the signature card designating CSO status. However, if a control agency's signature card designates CSO status, that status is valid for that control agency as well as any "controlled" agencies. Control/controlled agency relationships are defined by the CARS D09 Agency Descriptor Table. See CAPP Topic No. 70225, "Descriptor Tables."

500 General Coding Requirements - Security Table Maintenance Form

One Security Table Maintenance Form is completed for each <u>user identification number</u> to be established in the CARS security table. For the CARS Security Table, the user identification number will equal the ACF2 logon ID. All coding on the Security Table Maintenance Form must be accurate and legible. All codes should be printed in capital letters with appropriate spacing. Authorized input forms serve as the audit trail ensuring that entries were, in fact, the entries that were approved by the agency's CSO and DOA management.

All coding on the Security Table Maintenance Form must be carefully reviewed before submission to DOA. DOA will not correct errors or omissions on the form.

A sample of the Security Table Maintenance Form (DA-04-197) can be found in Exhibit 2.

Follow the procedures below when submitting Security Table Maintenance Forms to DOA for entry to CARS. Instructions are provided for each of the major components of the security table including the:

- Function
- User Identification
- Access Agencies
- Table Maintenance Functions
- Financial Data Functions
- Other Functions

500 General Coding Requirements - Security Table Maintenance Form (Continued)

501 Function

The function codes used to update the security table are:

A = Add a new user ID to the table

C = Change user ID in the table

D = Delete user ID from the table

502 User Identification Elements

The four elements which identify each user on both the Security Table Maintenance Forms and security table are the user identification number (user ID), user agency, user type, and user name.

User Identification Number

The USER ID is a seven position field that is the first element of the key to the security table. The USER ID must be entered left justified on both the security table maintenance screen and form. The USER ID is the logon ID that must have been previously established by submitting the Logon ID Request Form - IBM Technology in compliance with Subsection 600, "General Coding Requirements," which defines the logon ID.

User Agency

The USER AGENCY is a three position field that identifies the state agency with which the user is associated. The user agency is the other element that comprises the key to the security table. The agency code must be on the the D09 agency descriptor table.

User Type

The USER TYPE is a one position field that identifies and classifies the type of user. Valid values for user type are:

> 1 = Pre-Audit User
> 2 = DOA System Update
> 3 = DOA Data Entry
> 4 = Central Agency Inquiry
> 5 = Agency Inquiry
> 6 = Agency Data Entry or Error Correction Inquiry
> 7 = Agency Approval
> 8 = Agency Data Entry and Approval

Each user type is designed for specific access and capabilities within CARS. These capabilities are determined by several factors.

As outlined in Exhibit 4, each user type is restricted to certain input values for the various security table functions.

Exhibit 3 outlines the capabilities for those users whose Security Table data entry indicator is "U."

The CSO must limit requests for types 7 and 8 access to those individuals who appear on the agency's Authorized Signatories Form.

500 General Coding Requirements - Security Table Maintenance Form (Continued)

502 User Identification Elements (Continued)

User Name

USER NAME is a thirty-position field that contains the user's English name.

503 Access Agencies

The ACCESS AGENCIES component of the security table and form allows a maximum of 40 state agencies to be specified per user ID. For state agencies specified in this area the user may inquire into or update financial information. All agencies entered in this area must be on the D09 agency descriptor table, or the form will be returned. If the user is to be allowed access to all state agencies, the literal 'ALL' should be entered in the first agency field. The literal 'ALL' may be used for user types 1 through 4 only.

504 Table Maintenance Functions

The TABLE MAINTENANCE component of the security table allows the user to inquire into or update system tables. There are 44 table maintenance functions that may be independently specified for each user ID. The valid values for each of these 44 functions are:

<div align="center">

U = Update,
I = Inquiry, and
Blank = No access.

</div>

505 Financial Data Functions

The FINANCIAL DATA component of the security table consists of four elements. These elements are data entry, error correction, financial inquiry, and 1099 inquiry.

Data Entry Function

The DATA ENTRY function provides the user with the capability to enter or view financial transactions through the standard input screens. Valid values for the data entry indicator are:

<div align="center">

U = Update,
I = Inquiry, and
Blank = No access.

</div>

Exhibit 4 provides a detailed description of specific system functions, by user type, that are controlled by the data entry indicator.

500 General Coding Requirements - Security Table Maintenance Form (Continued)

505 Financial Data Functions (Continued)

Error Correction Function

The ERROR CORRECTION function allows the user to enter error corrections or view error transactions. Only DOA personnel can enter error correction transactions through the error correction screens. Valid values for the error correction indicator are:

$$U \quad = \quad \text{Update (DOA personnel only)},$$
$$I \quad = \quad \text{Inquiry, and}$$
$$\text{Blank} \quad = \quad \text{No access.}$$

Financial Inquiry Function

The FINANCIAL INQUIRY indicator allows the user to access the financial inquiry screens. Valid values for the financial inquiry indicator are:

$$Y \quad = \quad \text{Yes, and}$$
$$\text{Blank} \quad = \quad \text{No access.}$$

1099 Inquiry Function

The 1099 INQUIRY indicator allows the user to access the 1099 adjustment screens. Valid values for the 1099 inquiry indicator are:

$$Y \quad = \quad \text{Yes, and}$$
$$\text{Blank} \quad = \quad \text{No access.}$$

506 Other Functions

The OTHER FUNCTIONS component of the security table consists of six elements. These are report request, news screen, required edit option, forced entry indicator, reverse code, and modifier.

Report Request Function

The REPORT REQUEST INDICATOR allows the user to request standard reports. Valid values for the report request indicator are:

$$Y \quad = \quad \text{Yes, (DOA personnel only)},$$
$$\text{Blank} \quad = \quad \text{No access.}$$

500 General Coding Requirements - Security Table Maintenance Form (Continued)

506 Other Functions (Continued)

News Screen Function

The NEWS SCREEN INDICATOR allows the user to view or update the news broadcast screen with user defined messages. Valid values for the news screen indicator are:

Y = Yes, (DOA personnel only),
Blank = No Update, Inquiry only.

Required Edit Option Function

The REQUIRED EDIT OPTION INDICATOR specifies the lowest level of edit option that can be used by the user ID when financial transactions are entered through the on-line data entry screens. As batches are being created and transactions input into CARS, the operator must select from the following valid values for edit option: (See CAPP Topic No. 70230, "Data Entry.")

Blank = Data entry not allowed
A = Simple data entry
B = Data related editing

The security table's required edit option indicator operates as follows:

- If required edit option indicator is blank, the user cannot enter financial transactions.

- If required edit option indicator = A, the user may specify edit option A or B on input.

- If required edit option indicator = B, the user may specify edit option B on input.

Forced Entry Function - Not available in CARS at this time.

Reverse Code Function

The REVERSE CODE INDICATOR allows the user to input data into the reverse code field on detail transactions.

Y = Yes (DOA personnel only)
Blank = No Access

Modifier Function - Not available in CARS at this time.

500 General Coding Requirements - Security Table Maintenance Form (Continued)

507 Key for Agency Access to Tables

DESCRIPTOR TABLE

TABLE NUMBER	TABLE TITLE	AGENCY INQUIRY	UPDATE	PRINTOUT OF TABLE AVAILABLE (2)
01	Function	Yes	No	No
02	Sub-Function	Yes	No	No
03	Program	Yes	No(1)	No
04	Sub-Program	Yes	No(1)	No
05	Element	Yes	No	No
06	Fund	Yes	No	No
07	Fund Detail	Yes	No	Yes
08	Secretarial Area	Yes	No	No
09	Agency	Yes	No	No
10	Organizational Level 1	Yes	Yes	Yes
11	Organizational Level 2	Yes	Yes	Yes
12	Organizational Level 3	Yes	Yes	Yes
13	Organizational Level 4	Yes	Yes	Yes
14	GLA	Yes	No	No
15	Major Object	Yes	No(1)	No
16	Sub-Object	Yes	No(1)	No
17	Revenue Source	Yes	No	No
18	Project	Yes	Yes	Yes
19	Task	Yes	Yes	Yes
20	Phase	Yes	Yes	Yes
21	FIPS	Yes	No	No
22	Location Codes	Yes	No	Yes
23	Bank Codes	Yes	No	No
24	Payment Types	Yes	No	No
30	Pre-Audit	No	No	No
31	GAAP Fund	No	No	No
32	GAAP Sub-fund	No	No	No
33	CAFR Conversion	No	No	No
35	CDS	No	No	No

500 General Coding Requirements - Security Table Maintenance Form (Continued)

507 Key for Agency Access to Tables (Continued)

DESCRIPTOR TABLE (Continued)

TABLE NUMBER	TABLE TITLE	AGENCY INQUIRY	UPDATE	PRINTOUT OF TABLE AVAILABLE (2)
36	Revenue Class	Yes	No	No
37	Project Type	Yes	No	No
38	Subsidiary Account	Yes	No	No
39	Federal Catalog	Yes	No	No
40	Batch Type	Yes	No	No
41	Register Type	Yes	No	No
51	Error Code	Yes	No	No
52	Error Element	No	No	No
53	Va Power	Yes	No	Yes
	Transaction Code Decision Table	Yes	No	No
	Cost Code	Yes	Yes	Yes
	Vendor Edit	Yes	Yes	Yes
	Project Control	Yes	Yes	Yes
	Security	No	No	No
	Systems Management	No	No	No

Notes:

(1)   The Department of Planning and Budget (DPB) authorizes establishment of these specific codes, maintenance of related tables and use of these codes by agencies. Direct all inquiries to DPB.

(2)   Printouts for the indicated CARS tables are available through the following reports.

Report Name	Report Number
Descriptor Table Report	ACTR0900
Cost Code Table Report	ACTR0920
Project Control Table Report	ACTR0930
Vendor Edit Table Report	ACTR0940

(a)   These reports are issued upon request only. To request these reports, submit form DA-03-196, Standard Financial Report Request, to the Department of Accounts. See CAPP Topic No. 70260, "Reports," for submission procedures.

(b)   Descriptor Table Reports, ACTR0900, is available for individual tables. The table number must be included on the DA-03-196, Standard Financial Report Request. For example, an agency wanting a printout of project codes would request table D18. (See preceding list for descriptor table numbers.)

500 General Coding Requirements - Security Table Maintenance Form (Continued)

508 DOA Control Restrictions

Exhibit 4 provides a summary of the access allowed to each function by user type. DOA will audit each Security Table Maintenance Form (DA-04-197) by this summary.

Incorrectly prepared Security Table Maintenance Forms will be returned to the agency. DOA will not correct any errors or omissions on the form.

1. The form must be typed or legibly printed in ink.

2. All CARS edit criteria and agency restrictions on Security Table access must be met.

3. No erasures, correction fluid, correction tape, or other alterations may appear on the Security Table Maintenance Form.

4. For any changes to a given user ID in the security table, only the data to be changed should be entered on the Security Table Maintenance Form.

5. The top two copies of the form must be submitted to DOA.

6. Central agencies (e.g., Department of Planning and Budget) personnel may legitimately require access to agency data to an extent not allowed by the Security Table Maintenance Checklist. Any request for access beyond checklist restrictions should be made via a letter to accompany Form DA-04-197. This letter should be addressed to:

U. S. Mail	Other Delivery
Manager, General Accounting	Manager, General Accounting
DEPARTMENT OF ACCOUNTS	DEPARTMENT OF ACCOUNTS
P.O. Box 1971	101 N. 14th Street
Richmond, VA 23215-1971	Richmond, VA 23219

   The letter must include an itemized list of exceptions requested, with a justification for each exception, and be signed by the agency's CARS Security Officer (See Subsection 400, "CARS Security Officer.")

7. Users with Type 7 and Type 8 access must be on the agency's Authorized Signatories Form.

The Department of Accounts will strictly enforce its published restrictions on access to CARS functions through Security Table updates. However, each online agency will have considerable latitude, within DOA constraints, to enter, manipulate, and purge its own data. Each agency head must ensure that an effective agency-based internal control system exists to protect agency data.

This internal control system must be documented sufficiently to allow its examination by the Auditor of Public Accounts. DOA is not responsible for the existence, design, or function of such internal control systems.

600 Logon ID Request Form - IBM Technology (DIT03-001)

The DIT Logon ID Request Form - IBM Technology must be submitted before an agency requests on-line access to CARS. The form must be signed by the agency's ACF2 Security Officer, and then it must be processed by DIT (in the case of Inquiry logon IDs) or by both DOA and DIT (in the case of Data Entry logon IDs). The agency should not submit the Security Table Maintenance Form (DA-04-197) to General Accounting until the Logon ID Request Form - IBM Technology has been processed and the password has been changed for each logon ID.

The logon ID is the "key" required by an individual to gain access to CARS. The logon ID is the means by which the Department of Information Technology (DIT) identifies which agency is to be billed for computer usage. It may be necessary for a user to have more than on logon ID to access CARS. The Department of Accounts will pay for the computer processing costs accruing from the use of logon IDs which are assigned by DOA and begin with the abbreviation ACT. However, these logon IDs are limited to the following functions: financial data entry and updating the system tables. For this reason, the logon IDs assigned by DOA are known as "Data Entry" logon IDs. The user agency will be billed by DIT for the computer processing costs accruing from the use of logon IDs that are assigned by the user agency and begin with that agency's abbreviation. User agency logon IDs are allowed to perform all CARS function, including Table Inquiries and Financial Inqiury. For this reason, the logon IDs assigned by the agency are known as "Inquiry" logon IDs.

It is important to understand the difference between the DOA and agency responsibilities with respect to Data Entry and Inquiry logon IDs.

• Data Entry logon IDs are owned by DOA and are lent to the agency. DOA ACF2 Officers must establish, delete, and modify these logon IDs.

• Inquiry logon IDs are owned by the agency. The agency's ACF2 Officer must establish, delete, and modify these logon IDs.

Users must change their passwords promptly after new logon IDs have been established. To learn how to change a password, seek assistance from your agency's ACF2 Officer.

To establish an Inquiry logon ID, your ACF2 Officer must complete the Logon ID Request Form - IBM Technology in full and mail it to Computer Security Section, Department of Information Technology, Richmond Plaza Building, 110 S. 7th Street, 3rd Floor, Richmond, VA 23219. For instructions on how to fill out the form, the ACF2 Officer should consult the appropriate DIT publications, such as the DIT Customer Guide. DIT will establish the logon ID in COMPLETE and set initial security with the password equal to the logon ID and access suspended. The agency ACF2 officer must then unsuspend the logon ID, and the user must change the password, before the CARS Security Officer can submit the CARS Security Table Maintenance Form to DOA.

600 Logon ID Request Form - IBM Technology (DIT03-001) (Continued)

To establish a **Data Entry** logon ID, the agency ACF2 Security Officer should complete the Logon ID Request Form - IBM Technology in accordance with the following instructions:

Field	Definition
1) Logon ID	Leave this field blank.
2) Phone Number	Provide the **Phone Number of the Agency's ACF2 Officer**.
3) Name	Provide the User's Name.
4-9)	Leave these fields blank.
10) Special Considerations	Type or print the words, "FOR CARS ACCESS" and provide the name and address of the agency's ACF2 Officer. Stick-on labels may be used if desired.
11)	Leave this field blank.
12-14)	Agency ACF2 Officer signature and date. (DOA ACF2 Officer will countersign.)
14-19)	Leave these fields blank.

Mail the completed Data Entry logon ID form to either of the following addresses (DO NOT mail the form to DIT):

US Mail	Other Delivery
Manager, Data Base Administration Department of Accounts PO Box 1971 Richmond, VA 23215-1971	Manager, Data Base Administration Department of Accounts Second Floor, Monroe Building 101 N. 14th Street Richmond, VA 23219

700 Exhibits

The remainder of this topic consists of exhibits.These exhibits are presented to facilitate agency understanding of CARS Security.

Copies of the exhibits should not be sent to the Department of Accounts. These forms may not be reproduced from the exhibits. Blank forms using multiple pages of NCR paper may be obtained via written request from the DOA Director of Administrative Services.

Blank DIT forms may be obtained from the DIT Data Base Support Branch.

Exhibit 1

Form DA-04-197 (2-93)

COPY A: DOA COPY

Commonwealth Accounting and Reporting System/CARS
SECURITY TABLE MAINTENANCE FORM

To: Table Maintenance/General Accounting   Return to: _____
DEPARTMENT OF ACCOUNTS   _____
101 North 14th Street / P.O. Box 1971   _____
Richmond, VA 23215-1971   _____

From: Agency _____ Agency No. _____

I hereby request that you update the CARS Security Table as specified below. In conjunction with this request, I certify that this action conforms to all requirements for security table maintenance specified in the **Commonwealth Accounting Policies and Procedures Manual.** Further, I certify that this agency maintains a system of internal control over on-line access to CARS adequate to prevent unauthorized access to or changes in the data contained therein, and that the use of this form constitutes an integral part of that internal control system.

Name _____, CARS SECURITY OFFICER

Signature _____   Date _____

Function (A = Add, C = Change, D = Delete) [ ]   User ID [ ][ ][ ][ ][ ][ ][ ][ ]

User Agency [ ][ ][ ]   User Type [ ]

User Name [ ]

Access Agencies

Table Maintenance Functions (U = Update, I = Inquiry, Blank = Access Not Allowed)

Function	01	Org. Level 1	10	Task	19	CDS	35		
Subfunction	02	Org. Level 2	11	Phase/Year	20	Revenue Class	36		
Program	03	Org. Level 3	12	FIPS	21	Project Type	37		
Subprogram	04	Org. Level 4	13	PSD	22	Subsidiary Acct.	38		
Element	05	GLA	14	Bank Code	23	Federal Catalog	39		
Fund	06	Major Object	15	Payment Type	24	Batch Type	40		
Fund Detail	07	Minor Object	16	Pre-Audit	30	Register Type	41		
Secretarial	08	Revenue Source	17	GAAP Fund	31	Error Code	51		
Agency	09	Project	18	GAAP Subfund	32	Error Element	52		
				CAFR Conversion	33	VA Power Acct. No.	53		

Transaction Code [ ]   Cost Code [ ]   Vendor Edit [ ]   Project Control [ ]
Security [ ]   System Management [ ]

Financial Data Functions (U = Update, I = Inquiry, Blank = Access Not Allowed)

Data Entry [ ]   Error Correction [ ]   Financial Inquiry [ ]
1099 File Inquiry [ ]

Other Functions (Y = Yes, or blank = Not Allowed)

Report Request [ ]   News Screen [ ]   Required Edit Option [B]
Forced Entry [ ]   Reverse Code [ ]   Modifier [ ]

DEPARTMENT OF ACCOUNTS USE ONLY   The Security Table maintenance specified above

[ ] Meets requirements specified in the CAPP Manual and CARS edit criteria.
[ ] Does not meet CAPP Manual requirements and will be returned to agency.
[ ] Signature card verified.

_____   _____   _____
DOA Approval/Date   Data Entry by/Date   Verified by/Date

Exhibit 3
Access Allowed by User Type

The Security Table's data entry indicator has valid values of 'U' (Update), 'I' (Inquiry), and 'blank' (no access). The value 'U' actually grants a range of capabilities to the operator that depends on that operator's user type, elsewhere established in the operator's Security Table record.

The relationship between a data entry indicator = 'U' and the operator's access to CARS capabilities appears in the following table.

System Capabilities	User Types							
	1	2	3	4	5	6	7	8
• View batch headers	Y	Y	Y	*	*	Y	Y	Y
• View transactions	Y	Y	Y	*	*	Y	Y	Y
• Add batches	N	Y	Y	*	*	Y	N	Y
• Change batch headers	Y	Y	Y	*	*	Y	N	Y
• Delete batches	Y	Y	Y	*	*	Y	Y	Y
• Change batch status								
From　　　　To								
Agency Hold　　Agency Release	N	Y	N	*	*	N	Y	Y
Agency Release　Agency Hold	N	Y	N	*	*	N	Y	Y
Agency Release　Pre-Audit Hold	Y	N	N	*	*	N	N	N
Agency Release　Pre-Audit Release	Y	N	N	*	*	N	N	N
Pre-Audit Hold　Pre-Audit Release	Y	N	N	*	*	N	N	N
Pre-Audit Hold　Agency Hold	Y	Y	N	*	*	N	N	N
• Add transactions	Y	Y	Y	*	*	Y	N	Y
• Change transactions	Y	Y	Y	*	*	Y	N	Y
• Delete transactions	Y	Y	Y	*	*	Y	N	Y
• Change Vendor Payment Status	Y	Y	N	*	*	N	N	N

* Valid values for the data entry indicator for User Tyes 4 and 5 are confined to 'I' or 'blank'.

Exhibit 4
Security Table Maintenance Summary

The restrictions over a user type's access to CARS functions are summarized below. The section numbers are for reference when looking at Exhibit 1.

				User Type				
Item	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Section 1:
Agency Name
Agency Number   The elements
Signature   are required for
Date   all user types.

Section 2:

	1	2	3	4	5	6	7	8
Function			A, C or D for all user types.					
User ID	R(1)	R(1)	(R1)	R(2)	R(3)	R(3)	R(3)	R(3)
User Agency	997	997	151	R(6)	R	R	R	R
User Type	1	2	3	4	5	6	7	8
User Name	R	R	R	R	R	R	R	R
Access Agencies	(4)	(4)	(4)	(4)	(5)	(5)	(5)	(5)

       Legend:
         A = Add; C = Change;
         D = Delete; R = Required

Section 3:

	1	2	3	4	5	6	7	8
Function	I	U,I	I	I	I	I	I	I
Subfunction	I	U,I	I	I	I	I	I	I
Program	I	U,I	I	I	I	I	I	I
Subprogram	I	U,I	I	I	I	I	I	I
Element	I	U,I	I	I	I	I	I	I
Fund	I	U,I	I	I	I	I	I	I
Fund Detail	I	U,I	I	I	I	I	I	I
Secretarial Area	I	U,I	I	I	I	I	I	I
Agency	I	U,I	I	I	I	I	I	I
Organizational Level 1	I	U,I	I	I	I	U,I	I	U,I
Organizational Level 2	I	U,I	I	I	I	U,I	I	U,I
Organizational Level 3	I	U,I	I	I	I	U,I	I	U,I
Organizational Level 4	I	U,I	I	I	I	U,I	I	U,I
General Ledger Account	I	U,I	I	I	I	I	I	I
Major Object	I	U,I	I	I	I	I	I	I
Minor Object	I	U,I	I	I	I	I	I	I
Revenue Source	I	U,I	I	I	I	I	I	I
Project	I	U,I	I	I	I	U,I	I	U,I
Task	I	U,I	I	I	I	U,I	I	U,I
Phase	I	U,I	I	I	I	U,I	I	U,I
FIPS	I	U,I	I	I	I	I	I	I
Political Subdivision (PSD)	I	U,I	I	I	I	I	I	I

Exhibit 4 (Continued)

Item	User Type							
	1	2	3	4	5	6	7	8
Bank Code	I	U,I	I	I	I	I	I	I
Payment Type	I	U,I	I	I	I	I	I	I
Pre-Audit Hold	U,I							
GAAP Fund		U,I						
GAAP Subfund		U,I						
CAFR Conversion		U,I						
Comptroller's Debt Set-Off		U,I						
Revenue Class	I	U,I	I	I	I	I	I	I
Project Type	I	U,I	I	I	I	I	I	I
*Subsidiary Accounts		U,I	I	I	I	I	I	I
Federal Catalog No.	I	U,I	I	I	I	I	I	I
Batch Type	I	U,I	I	I	I	I	I	I
Register Type	I	U,I	I	I	I	I	I	I
Error Code	I	U,I	I	I	I	I	I	I
Error Element		U,I						
Virginia Power	I	U,I	I	I	I	I	I	I
Transaction Code	I	U,I	I	I	I	I	I	I
Cost Code	I	U,I	I	I	I	U,I	I	U,I
Vendor Edit	I	U,I	I	I	I	U,I	I	U,I
Project Control	I	U,I	I	I	I	U,I	I	U,I
Security		U,I						
System Management	I	U,I	I	I				
Data Entry	U,I	U,I	U	I	I	U	U	U
Error Correction	I	U,I	I	I	I	I	I	I

Legend:
U = Update; I = Inquiry;
Any element may be left blank; blank allows no access. Items above with no indicator must be blank.

Section 4:

Item	1	2	3	4	5	6	7	8
Financial Inquiry	Y	Y	Y	Y	Y	Y	Y	Y
1099 Inquiry		Y			Y	Y	Y	Y
Report Request		Y						
*Ad Hoc Reports								
News Screen		Y						
Required Edit Option	B	A,B	A			B		B
Reverse		Y						
*Modifier								

Legend:
Y = Yes (inquiry allowed); Blank = Not allowed
A, B = Required Edit Option Indicators
* = Function not available in CARS at this time
Any element may be left blank. Items above with no indicator must be blank.

Notes:
1   User ID prefix must be ACT
2   User ID prefix must be ACT if Agency = 997; otherwise prefix must not = ACT
3   User ID prefix must not = ACT if any indicators are set as I or Y
4   Can equal 'ALL' or from 1 to 40 individual agencies from D09 table.
5   Must = User Agency. If user agency is a control agency, access agencies may include controlled agencies.
6   Must = 122, 133, 150 or 997.

800 Internal Control

The control of an agency's access to CARS is vital. The CARS Security Officer is responsible for a comprehensive system of internal control over both on-line and off-line access to CARS tables and files. This access control is vital to ensure the integrity of accounting transactions submitted to CARS.

900 Records Retention

Security Table Maintenance Forms must be retained for three (3) years or until audited by the Auditor of Public Accounts, whichever is longer.

1000 DOA Contacts

Manager, General Accounting, (804) 225-2244

Manager, Data Base Administration, (804) 225-3054

1100 Subject Cross References

CAPP Topic No. 20310, "Expenditures"

CAPP Topic No. 70225, "Descriptor Tables"

CAPP Topic No. 70230, "Data Entry"

CAPP Topic No. 70260, "Reports"